

Amendments to the Claims:

Please amend the claims as follows. The following listing of claims will replace all prior versions of the claims in the application.

Listing of Claims

1. (Currently amended) An encryption method for dividing a first plaintext bit stream of length $2n$ into first and second sub-bit streams of length n , dividing a second plaintext bit stream of length $2n$ into third and fourth sub-bit streams of length n , and generating a ciphertext bit stream of length $2n$ from the first, second, third and fourth sub-bit streams using 2-rounds of encryption, the method comprising the steps of:

performing ~~a~~the first-round of encryption by encrypting the received the first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting the second ciphertext bit stream encrypted again with a predetermined time delay right after the first ciphertext bit streams of length n are outputted;

generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream at the same time of performing encryption of the second ciphertext bit stream;

generating a second operated ciphertext bit stream by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream; and

performing ~~a~~the second-round of encryption by encrypting the received first operated ciphertext bit stream and the second operated ciphertext bit stream, comprising the predetermined time delay, with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n after encrypting the first operated ciphertext bit stream again with predetermined second encryption codes.

2. (Previously presented) The encryption apparatus of claim 1, wherein the predetermined first encryption codes comprises at least one of KO_{1,1}, KO_{1,2}, KO_{1,3}, KI_{1,1}, KI_{1,2}, and KI_{1,3}.

3. (Previously presented) The encryption apparatus of claim 1, wherein the predetermined second encryption codes comprises at least one of KO_{2,1}, KO_{2,2}, KO_{2,3}, KI_{2,1}, KI_{2,2}, and KI_{2,3}.

4. (Previously presented) The encryption method of claim 2, wherein the first-round encryption step comprises the steps of:

generating a first signal by performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO_{1,1} to provide a first exclusive-OR operated bitstream, encrypting the first exclusive-OR-operated bit stream with the first encryption code KI_{1,1} to provide a first encrypted signal, and performing a logical exclusive-OR operation on the first encrypted signal and the second sub-bit stream delayed by time required for the encryption;

generating the first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second sub-bit stream and the first encryption code KO_{1,2}, to provide a second exclusive-OR operated bitstream[[,]] encrypting the second exclusive-OR-operated bit stream with the first encryption code KI_{1,2} to provide a second encrypted signal, and performing a logical exclusive-OR-operation on the second encrypted signal and the first signal;

generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first signal and the first encryption code KO_{1,3} to provide a third exclusive-OR operated bitstream, encrypting the third exclusive-OR-operated bit stream with the first encryption code KI_{1,3}, and performing a logical exclusive-OR-operation on the encrypted signal with the first sub-bit stream delayed by time required for the encryption.

5. (Previously presented) The encryption method of claim 3, wherein the second-round encryption step comprises the steps of:

generating a second signal by performing a logical exclusive-OR-operation on the first operated ciphertext bit stream and the second encryption code $KO_{2,1}$ to provide a fourth exclusive-OR operated bitstream, encrypting the fourth exclusive-OR-operated bit stream with the second encryption code $KI_{2,1}$ to provide a third encrypted signal, performing a logical exclusive-OR-operation on the third encrypted signal and the second operated ciphertext bit stream to provide a fifth exclusive-OR operated bitstream;

generating the third operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second operated ciphertext bit stream and the second encryption code $KO_{2,2}$, encrypting the fifth exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$ to provide a fourth encrypted signal, and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal delayed by time required for the encryption; and

generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the second encryption code $KO_{2,3}$ encrypting the sixth exclusive-OR-operated bit stream with the second encryption code $KI_{2,3}$, and performing a logical exclusive-OR-operation on the encrypted signal with the third operated ciphertext bit stream.

6. (Original) The encryption method of claim 5, wherein each of the encryptions includes first and second sub-encryptions, and outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal.

7. (Original) The encryption method of claim 5, wherein a 16-bit input bit stream is divided into a 9-bit stream and a 7-bit stream, a 9-bit ciphertext bit stream is generated from the 9-bit stream using a first equation, and a 7-bit ciphertext bit stream is generated from

Amendment filed June 19, 2008
Responding to Office Action mailed February 21, 2008
App. Serial No. 10/679,391

the 7-bit stream using a second equation in each of the sub-encryptions, wherein said first equation comprises

$$\begin{aligned}y_0 &= (x_0x_2) \oplus x_3 \oplus (x_2x_5) \oplus (x_5x_6) \oplus (x_0x_7) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_4x_8) \oplus (x_5x_8) \oplus (x_7x_8) \oplus '1'; \\y_1 &= x_1 \oplus (x_0x_1) \oplus (x_2x_3) \oplus (x_0x_4) \oplus (x_1x_4) \oplus (x_0x_5) \oplus (x_3x_5) \oplus x_6 \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_5x_8) \oplus '1'; \\y_2 &= x_1 \oplus (x_0x_3) \oplus (x_3x_4) \oplus (x_0x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_5x_6) \oplus (x_4x_7) \oplus (x_5x_7) \oplus (x_6x_7) \oplus x_8 \oplus (x_0x_8) \oplus '1'; \\y_3 &= x_0 \oplus (x_1x_2) \oplus (x_0x_3) \oplus (x_2x_4) \oplus x_5 \oplus (x_0x_6) \oplus (x_1x_6) \oplus (x_4x_7) \oplus (x_0x_8) \oplus (x_1x_8) \oplus (x_7x_8); \\y_4 &= (x_0x_1) \oplus (x_1x_3) \oplus x_4 \oplus (x_0x_5) \oplus (x_3x_6) \oplus (x_0x_7) \oplus (x_6x_7) \oplus (x_1x_8) \oplus (x_2x_8) \oplus (x_3x_8); \\y_5 &= x_2 \oplus (x_1x_4) \oplus (x_4x_5) \oplus (x_0x_6) \oplus (x_1x_6) \oplus (x_3x_7) \oplus (x_4x_7) \oplus (x_6x_7) \oplus (x_5x_8) \oplus (x_6x_8) \oplus (x_7x_8) \oplus '1'; \\y_6 &= x_0 \oplus (x_2x_3) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_4x_5) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus x_7 \oplus (x_1x_8) \oplus (x_3x_8) \oplus (x_5x_8) \oplus (x_7x_8); \\y_7 &= (x_0x_1) \oplus (x_0x_2) \oplus (x_1x_2) \oplus x_3 \oplus (x_0x_3) \oplus (x_2x_3) \oplus (x_4x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_2x_7) \oplus (x_5x_7) \oplus x_8 \oplus '1'; \\y_8 &= (x_0x_1) \oplus x_2 \oplus (x_1x_2) \oplus (x_3x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_4x_6) \oplus x_7 \oplus (x_2x_8) \oplus (x_3x_8);\end{aligned}$$

and said second equation comprises

$$\begin{aligned}y_0 &= (x_1x_2) \oplus x_3 \oplus (x_1x_4) \oplus x_5 \oplus (x_2x_5) \oplus (x_3x_4) \oplus (x_1x_6) \oplus (x_2x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_4x_8) \oplus (x_5x_8) \oplus (x_7x_8); \\y_1 &= (x_0x_2) \oplus (x_1x_3) \oplus (x_2x_4) \oplus x_5 \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_6x_7) \oplus '1'; \\y_2 &= x_1 \oplus (x_1x_3) \oplus (x_2x_4) \oplus (x_1x_5) \oplus (x_3x_5) \oplus (x_1x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_6x_7) \oplus (x_7x_8) \oplus '1'; \\y_3 &= x_1 \oplus (x_1x_2) \oplus (x_1x_4) \oplus (x_1x_5) \oplus (x_3x_5) \oplus (x_1x_6) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_4x_8) \oplus (x_1x_8); \\y_4 &= (x_1x_2) \oplus x_3 \oplus (x_1x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_2x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_4x_8) \oplus (x_5x_8) \oplus (x_7x_8) \oplus '1'; \\y_5 &= x_2 \oplus (x_1x_3) \oplus (x_1x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_6x_7) \oplus (x_7x_8) \oplus '1'; \\y_6 &= (x_1x_2) \oplus (x_1x_3) \oplus (x_1x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_6x_7) \oplus (x_7x_8) \oplus '1'; \\y_7 &= (x_1x_2) \oplus (x_1x_3) \oplus (x_1x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_6x_7) \oplus (x_7x_8) \oplus '1'; \\y_8 &= (x_1x_2) \oplus (x_1x_3) \oplus (x_1x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_6x_7) \oplus (x_7x_8) \oplus '1';\end{aligned}$$

8. (Previously presented) An encryption apparatus for dividing a first plaintext bit stream of length $2n$ into first and second sub-bit streams of length n , dividing a second plaintext bit stream of length $2n$ into third and fourth sub-bit streams of length n , and generating a ciphertext bit stream of length $2n$ from the first, second, third and fourth sub-bit streams using 2-rounds of encryption, the apparatus comprising:

a first ciphering unit for receiving the first and second sub-bit streams, and generating first and second ciphertext bit streams of length n by encrypting the first and second sub-bit streams with predetermined first encryption codes KO_{1,1}, KO_{1,2}, KO_{1,3}, KI_{1,1}, KI_{1,2}, and KI_{1,3} an odd number of times, and the second ciphertext bit stream encrypted again with a predetermined time delay after the first ciphertext bit streams of length n are outputted;

an operating unit for generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream at the same time of performing the first-round of encryption, and generating a second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second ciphertext bit stream with the fourth sub-bit stream; and

a second ciphering unit for receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream comprising the predetermined time delay, generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined second encryption codes KO_{2,1}, KO_{2,2}, KO_{2,3}, KI_{2,1}, KI_{2,2}, and KI_{2,3} an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams after encrypting the first operated ciphertext bit stream again with predetermined second encryption codes.

9. (Previously presented) The encryption apparatus of claim 8, wherein the first ciphering unit comprises:

a first block comprising a first exclusive-OR operator for performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO_{1,1}, a first sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI_{1,1}, and a second exclusive-OR operator for generating a first signal by performing a logical exclusive-OR operation on the encrypted signal with the second sub-bit stream being delayed to provide time for the encryption;

a second block comprising a third exclusive-OR operator for performing a logical exclusive-OR operation on the second sub-bit stream and the first encryption code KO_{1,2}, a

second sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code $KI_{1,2}$, and a fourth exclusive-OR operator for generating the first operated ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the first signal; and

a third block comprising a fifth exclusive-OR operator for performing a logical exclusive-OR operation on the first signal and the first encryption code $KO_{1,3}$, a third sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code $KI_{1,3}$, and a sixth exclusive-OR operator for generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the first sub-bit stream delayed by time required for the encryption.

10. (Previously presented) The encryption apparatus of claim 8, wherein the second ciphering unit comprises:

a fourth block comprising a seventh exclusive-OR operator for exclusive-OR-operating the first operated ciphertext bit stream with the second encryption code $KO_{2,1}$, a fourth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,1}$, and an eighth exclusive-OR operator for generating a second signal by performing a logical exclusive-OR-operation on the encrypted signal and the second operated ciphertext bit stream;

a fifth block comprising a ninth exclusive-OR operator for exclusive-OR-operating the second operated ciphertext bit stream with the second encryption code $KO_{2,2}$, a fifth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption code $KI_{2,2}$, and a tenth exclusive-OR operator for generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the second signal delayed by time required for the encryption; and

a sixth block comprising an eleventh exclusive-OR operator for performing a logical exclusive-OR operation on the second signal with the second encryption code $KO_{2,3}$, a sixth sub-cipher for encrypting the exclusive-OR-operated bit stream with the second encryption

code KI_{2,3}, and a twelfth exclusive-OR operator for generating the fourth ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the third ciphertext bit stream.

11. (Previously presented) The encryption apparatus of claim 10, wherein each of the first to sixth sub-ciphers includes first and second sub-ciphering units, and a register for storing the outputs of the first and second sub-ciphering units and simultaneously retrieving the outputs according to an external clock signal.

12. (Original) The encryption apparatus of claim 11, wherein each of the first and second sub-ciphering units divides a 16-bit input bit stream into a 9-bit stream and a 7-bit stream, and generates a 9-bit ciphertext bit stream from the 9-bit stream using a third equation, and a 7-bit ciphertext bit stream from the 7-bit stream using a fourth equation, said third equation comprising

$$\begin{aligned}y_0 &= (x_0x_2) \oplus x_3 \oplus (x_2x_5) \oplus (x_5x_6) \oplus (x_0x_7) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_4x_8) \oplus (x_5x_8) \oplus (x_7x_8) \oplus '1'; \\y_1 &= x_1 \oplus (x_0x_1) \oplus (x_2x_3) \oplus (x_0x_4) \oplus (x_1x_4) \oplus (x_0x_5) \oplus (x_3x_5) \oplus x_6 \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_5x_8) \oplus '1'; \\y_2 &= x_1 \oplus (x_0x_3) \oplus (x_3x_4) \oplus (x_0x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_5x_6) \oplus (x_4x_7) \oplus (x_5x_7) \oplus (x_6x_7) \oplus x_8 \oplus (x_0x_8) \oplus '1'; \\y_3 &= x_0 \oplus (x_1x_2) \oplus (x_0x_3) \oplus (x_2x_4) \oplus x_5 \oplus (x_0x_6) \oplus (x_1x_6) \oplus (x_4x_7) \oplus (x_0x_8) \oplus (x_1x_8) \oplus (x_7x_8); \\y_4 &= (x_0x_1) \oplus (x_1x_3) \oplus x_4 \oplus (x_0x_5) \oplus (x_3x_6) \oplus (x_0x_7) \oplus (x_6x_7) \oplus (x_1x_8) \oplus (x_2x_8) \oplus (x_3x_8); \\y_5 &= x_2 \oplus (x_1x_4) \oplus (x_4x_5) \oplus (x_0x_6) \oplus (x_1x_6) \oplus (x_3x_7) \oplus (x_4x_7) \oplus (x_6x_7) \oplus (x_5x_8) \oplus (x_6x_8) \oplus (x_7x_8) \oplus '1'; \\y_6 &= x_0 \oplus (x_2x_3) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_4x_5) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus x_7 \oplus (x_1x_8) \oplus (x_3x_8) \oplus (x_5x_8) \oplus (x_7x_8); \\y_7 &= (x_0x_1) \oplus (x_0x_2) \oplus (x_1x_2) \oplus x_3 \oplus (x_0x_3) \oplus (x_2x_3) \oplus (x_4x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_2x_7) \oplus (x_5x_7) \oplus x_8 \oplus '1'; \\y_8 &= (x_0x_1) \oplus x_2 \oplus (x_1x_2) \oplus (x_3x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_4x_6) \oplus x_7 \oplus (x_2x_8) \oplus (x_3x_8);\end{aligned}$$

and said fourth equation comprising

Amendment filed June 19, 2008
Responding to Office Action mailed February 21, 2008
App. Serial No. 10/679,391

y0-(x1x2)⊕x1(⊕(x1x1x1)⊕x2⊕(x2x2))⊕(x1x1x1)⊕x2⊕(x1x1)⊕(x1x1x1)⊕(x1x1x1);
y1-(x1x2)⊕(x1x2)⊕(x1x2)⊕x2⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1);
y2-x1(⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1));
y3-x1(⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1)⊕(x1x1x1));
y4-(x1x2)⊕x2⊕(x1x2)⊕(x1x2)⊕(x1x2x1)⊕(x1x2)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1);
y5-x2⊕(x1x2)⊕(x1x2)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1);
y6-(x1x2)⊕(x1x2x1)⊕(x1x2)⊕(x1x2)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1)⊕(x1x2x1);